

REMARKS

In the specification, various paragraphs have been amended to correct minor editorial problems as indicated by the Examiner in paragraph one of the Office Action. Applicants respectfully submit that all such objections have been obviated pursuant to these corrections.

In paragraph two of the Office Action, the Examiner objected to claims 3 and 12 of the present application again for minor grammatical errors. Applicants respectfully submit that such errors now have been corrected via the present amendment.

Applicants further acknowledge that claims 21-50 of the present application were inadvertently mis-numbered and, as stated by the Examiner, should have been properly numbered 19-48. Applicants respectfully submit that the listing of claims which accompanies the present amendment accurately reflects the correct numbering of these claims from 19-48.

The Examiner further rejected claims 28-30 and 43-45 under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. To summarize, the Examiner stated that Applicants disclose methods and arrangements "whereupon digital data is grouped into data segments and furthermore the data segments have no ties to a specific ordering... however, segments without any ties to a specific ordering are essentially independent data and obviate a means for ordering the segments to re-establish the original digital data." Applicants respectfully submit that all of the aforementioned claims which were rejected under 35 U.S.C. §112, have now been amended so as to eliminate the reference to a specific ordering.

Accordingly, Applicants respectfully request that the §112 rejections be withdrawn at this time.

The Examiner has rejected, in particular, independent claims 1-3 and 10-12 of the present application under 35 U.S.C. §102(a) as being unpatentable in view of the article by Halsall entitled "Data Communications, Computer Networks and Open System 4th Edition." Details of such rejection will not be reiterated here.

Applicants specifically wish to point out, however, that the Examiner has extracted information from two entirely different chapters of the Halsall article to formulate his novelty rejection. Indeed, Chapter 3.4 is initially referenced as disclosing a method whereby a segment checksum is formed for data segments of digital data which is grouped in data segments. Based on the commutative linking of such segment checksums, a commutative checksum is formed.

Transmission errors are then determined on the basis of this commutative checksum. Thereafter, the Examiner cites 12.4 of the Halsall article which discloses an altogether different (known) method for encoding text, whereby non-encoded text is encoded by using a cryptographic operation. By piecing together all of the various bits of information disclosed in Halsall, the Examiner determines that all of the elements of each of the independent claims of the present application are disclosed.

Applicants respectfully submit that this conclusion is erroneous given that the two methods described above are directed to entirely different objects such that someone skilled in this field of art would never consider such a combination. The first method disclosed in Halsall already fulfills the respective object to be solved; i.e., the recognition of transmission errors. As such, someone skilled in this field of art would have no reason to consider expanding such a method by an encoding method which has nothing in common with a checksum and a recognition of transmission errors. Moreover, the second method of Halsall suggests an encoding of a non-encoded, plain text whereas the first method ends with a sum; i.e., commutative checksum. Someone skilled in this field of art would have no reason to employ a method for encoding text with respect to the arrived-at sum, when the object of the method is already achieved by the sum.

Applicants respectfully submit that the Halsall article does not teach or suggest, nor even contemplate, a single method which combines the formation of a checksum with respect to data segments with a commutative linking of the checksums and, in a further combination, with a cryptographic encoding of the commutatively linked checksums. Only through this commutative linking of segment checksums is it possible to check a data stream independently of a sequence of the data packets in the data stream. Thus, regardless of the sequence of the data packets, a commutative linking of the individual segment checksums with respect to a commutative checksum independently of their linking sequence provides the same checkable value to be compared; i.e., the commutative checksum. It is therefore guaranteed by the forming of the checksum and by its subsequent commutative linking that the commutative checksum always receives the same value regardless of the sequence of the data segments. Furthermore, the present invention as claimed also provides a cryptographic securing of the linking result. This

result. This further increases the security of the inventive method whereby the checksum is protected against manipulations.

In light of the above, Applicants respectfully submit that independent claims 1-3 and 10-12 of the present application, as well as claims 19-48 which respectively depend therefrom, are both novel and non-obvious over the art of record. Accordingly, Applicants respectfully request that a timely Notice of Allowance be issued in this case.

It is further acknowledged that a one-month extension of time (\$110.00) is due in connection with this Amendment. However, if any additional fees are due in connection with this application as a whole, the Examiner is authorized to deduct said fees from Deposit Account No.: 02-1818. If such a deduction is made, please indicate the attorney docket number (0112740-466) on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY 

William E. Vaughan

Reg. No. 39,056

P.O. Box 1135

Chicago, Illinois 60690-1135

Phone: (312) 807-4292

Dated: December 15, 2003